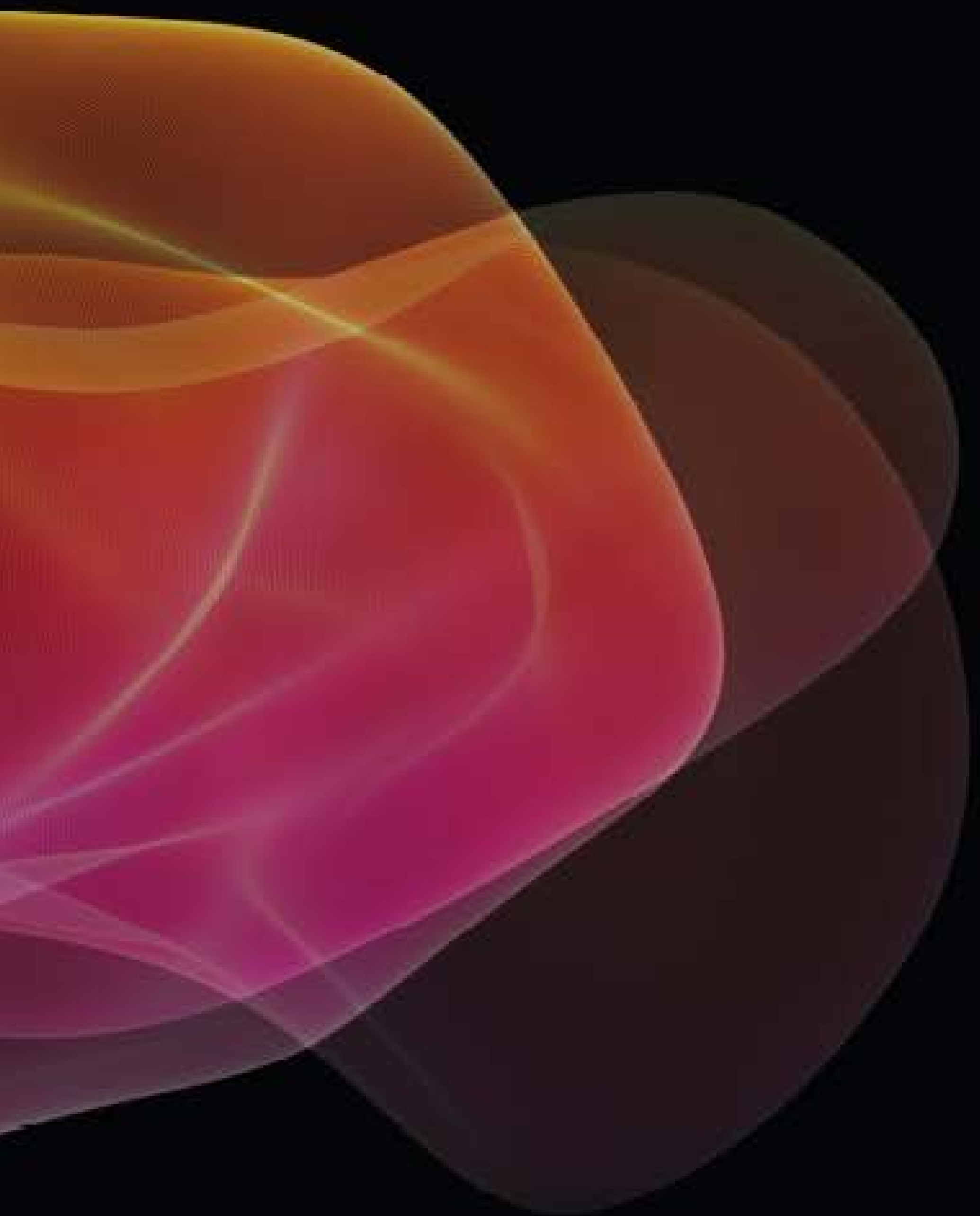
MORPHISEC
Moving Target Defense



The Five Major Security Pitfalls of Working from Home

And How to Solve Them

INTRODUCTION

There was a time when working remotely was limited to outside sales reps and independent contractors. That reality has shifted dramatically in even the last five years, with more workers in more industries working from home all or most of the time.

According to Owl Labs, who surveyed more than 1,200 American workers between the ages of 22 and 65 in 2019, 62 percent of employees work remotely at any frequency and 38 percent of American workers are full-time on-site employees. Of the people who work remotely, 54 percent of employees around the world report working from home at least once per month, with 48 percent working from home at least once per week, and 30 percent always working from home. This is across industries and job titles, whereas only a few years ago the only people working from home were outside sales reps or independent contractors.

The outbreak of COVID-19 accelerated this trend, forcing many employers to make most or all of their employees suddenly work from home, often using their personal computers for business tasks. Highmark Health, for example, told all 8,000 of its employees to work from home and Facebook informed all of its 46,000 employees that they should do the same. Many companies are now in similar situations, faced with an external factor that accelerated the existing trend of remote work.

13% of remote employees can't access their corporate network, so they send emails to customers and coworkers from their personal machines

Source: IndusFace

With more people working remotely than ever before

Regardless of the reason, CISOs must craft a flexible security architecture to ensure that those long-term or newly remote workers can access the software they need to do their job in a secure environment. These remote employees thus create additional operational challenges and security risks for the IT department to manage, including:

1

UNSECURED AND UNRELIABLE HOME NETWORKS

2

INCREASED RISK OF REMOTE WORK APPLICATION EXPLOITS, BROWSER-BASED ATTACKS, AND SOCIAL ENGINEERING

3

INABILITY TO REMEDIATE SECURITY INCIDENTS ON REMOTE WORKSTATIONS

4

HEIGHTENED RELIANCE ON ENDPOINT PROTECTION SOFTWARE

5

INABILITY TO HARDEN AND ENSURE PROPER IT HYGIENE ON HOME COMPUTERS

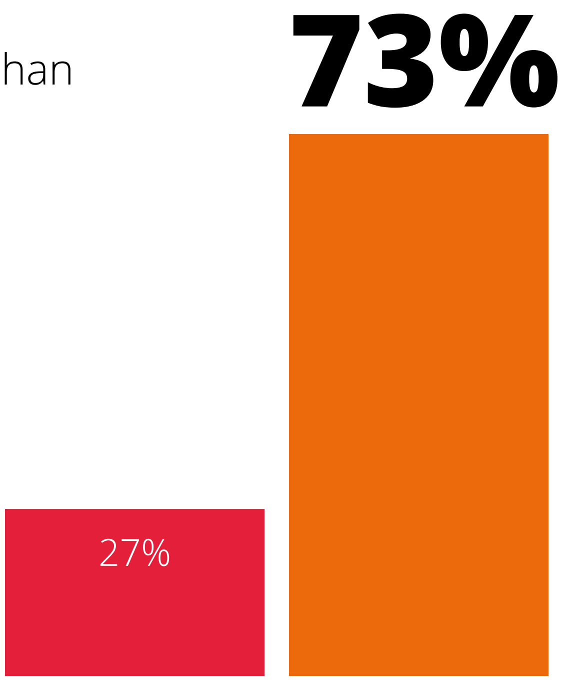
This ebook will cover these five major security pitfalls facing remote employees and how CISOs can work to solve them

UNSECURED AND UNRELIABLE HOME NETWORKS

The modern enterprise leverages a stack of network security tools and security-focused hardware at the perimeter to minimize the amount of malware that can even reach the endpoint. These include firewalls, secure gateways, network mappers, port scanners, and packet analyzers.

Home networks are inherently less secure than corporate networks. They lack the network security solutions that corporate IT teams deploy on enterprise systems for an additional layer of protection. As a result of the lack of advanced security tools, the reality of home networks is that they are far less secure than corporate ones.

Home networks are also less reliable than corporate networks. There's no IT team monitoring the network to ensure that your remote employee has a reliable connection to the internet. This manifests in employees not being able to access their corporate networks; 13 percent of remote employees admit that they cannot connect to their corporate networks, so they send business email to customers, partners, and co-workers via their personal email instead.



of IT leaders say remote employees are a bigger security risk than on-site workers

Source: OpenVPN

HOW MOVING TARGET DEFENSE FIXES THE PROBLEM

A combination of traditional antivirus with an advanced solution like moving target defense secures your remote employees against cyberattacks even in an unsecured and unreliable home network. With moving target defense from Morphisec, paired with built-in Windows Defender AV, your employees have the tight security they need to work without relying on network tools that are meant to ensure those attacks never reach the endpoint in the first place

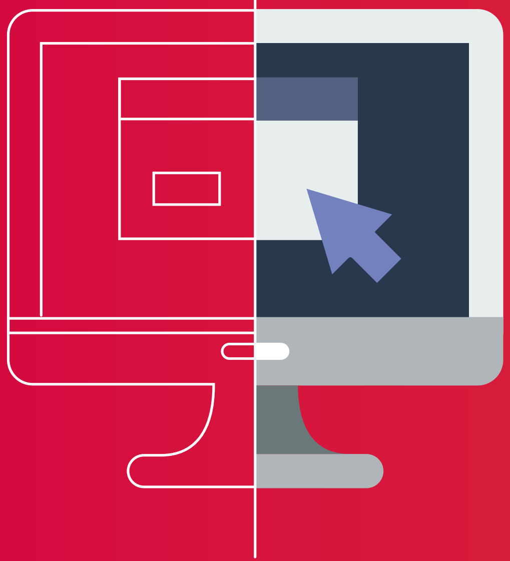
The Morphisec platform's performance also doesn't rely on or degrade internet connectivity. Because our software doesn't require access to the internet to update a signature database, unreliable networks aren't a barrier to ensuring that your employee's endpoints are protected. This includes protection for computers that are offline because of network connection issues.

MORPHISEC + Microsoft

INCREASED RISK OF REMOTE WORK APPLICATION EXPLOITS, BROWSER-BASED ATTACKS, AND SOCIAL ENGINEERING

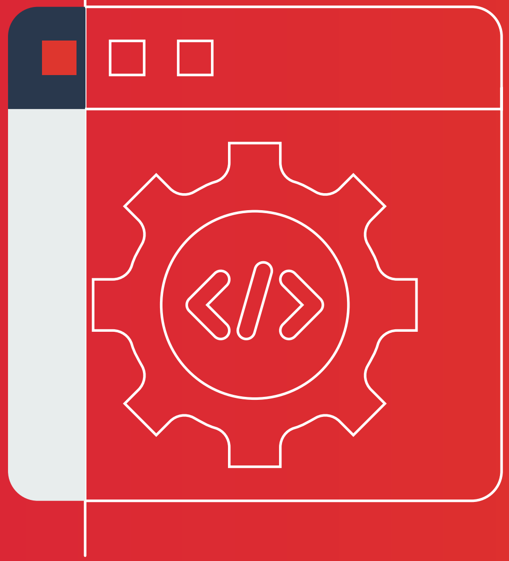
Web-based threats leverage browsers and their extensions, websites, content management systems, and IT components of web services and applications to harvest credentials, skim visitor payment details, or infect systems with malware or ransomware (or any combination thereof). Of particular danger to organizations are fileless attacks that take advantage of browser third-party tools, as there are no links or files for security systems to detect and behavioral monitoring always leaves some window of exposure.

Remote work applications like those used for virtual meetings and screen sharing are proliferating, which increases the attack surface for those who use them. We anticipate an increase in exploits for these tools as they have high privileges and can be leveraged for remote code execution. Furthermore, these create an opportunity for social engineering, as invites for these can be spoofed for phishing attempts.



50% of web applications contain high vulnerabilities

Source: Positive Technologies



84% of browser vulnerabilities are due to a security misconfiguration

Source: Positive Technologies

HOW MOVING TARGET DEFENSE FIXES THE PROBLEM

Browser-based attacks, remote work application exploits, and phishing attempts can be resolved through several vehicles, such as with multi-factor authentication and moving target defense solutions that secure your remote workers' browser against advanced evasive malware.

The Morphisec Unified Threat Prevention Platform adds a dedicated memory defense layer to every browser instance as a guard against these attack vectors. As a result, these attacks are unable to gain a foothold within the remote worker's machine.

INABILITY TO REMEDIATE SECURITY INCIDENTS ON REMOTE WORKSTATIONS

The standard practice for remediating security incidents is to walk a computer over to the IT or security team and have them reimage a machine to resolve any malware. This can't happen with a remote employee, especially in situations where they are physically unable to have an in-person visit with the IT team. Even the remote shell functionality of many endpoint detection and response products, which could solve this problem, requires that the infected machine remain powered and online, which is not ideal and sometimes an impossibility.

This means a successful attack on a remote employee can cost even more in lost time because they have to figure out a way to connect with remote IT staff who might possibly be able to resolve the issue. Moreover, endpoint detection and response products need to be constantly feeding data back to a central system for review. Most enterprises will not be able to roll out these types of solutions to personal computers, and even if they could, there are concerns with private data being shared with these businesses.

The average security breach costs

$8.94M

Source: Ponemon Institute

HOW MOVING TARGET DEFENSE FIXES THE PROBLEM

To resolve the issue of remediating security incidents remotely, you need to deploy a solution that focuses on prevention instead of detection and response. Pairing the Morphisec Unified Threat Prevention Platform with Microsoft Windows Defender AV (standard on all Windows 10 machines) creates the perfect prevention environment to automatically stop attacks.

Windows Defender AV is one of the best antivirus solutions on the market, and the Morphisec platform automatically blocks the attacks that bypass Defender. These two products combined result in a strong footprint that prevents attacks so there's no need to remediate and nothing to try sending back via an EDR platform.

MORPHISEC + Microsoft

4

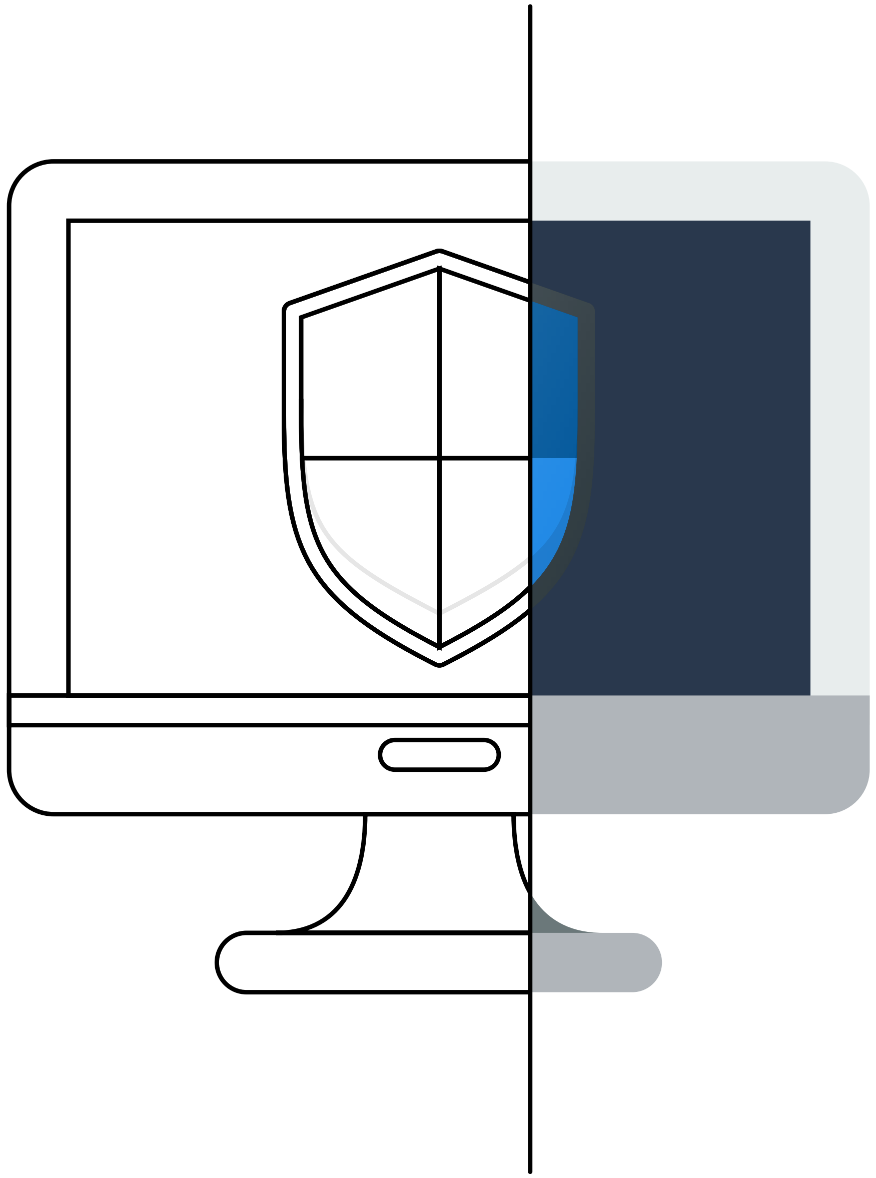
HEIGHTENED RELIANCE ON ENDPOINT PROTECTION SOFTWARE

On the home network, aside from basic firewalls, the endpoint is the first and last line of defense against cyberattack. This can be either the home computer or your employee's company-owned laptop. The point is that they lack the security of additional monitoring and protection tools on the corporate network that secures critical systems from damaging attacks.

This results in additional strain on signature-based, client-grade antivirus software. Although antivirus products do very well at protecting against file-based malware, fileless malware bypasses these products because there is no signature to detect.

Antivirus software missed 60% of attacks in 2019

Source: Ponemon Institute



HOW MOVING TARGET DEFENSE FIXES THE PROBLEM

Enterprises need to deploy additional solutions onto their employee's remote workstations to protect against fileless attacks. The Morphisec Unified Threat Prevention Platform morphs application memory to prevent fileless attacks, evasive malware, zero days, and in-memory exploits from gaining a foothold in the endpoint.

With Morphisec deployed on every remote employee's endpoint alongside the antivirus solution, workstations are secured against the most damaging cyberattacks.

INABILITY TO HARDEN AND ENSURE PROPER IT HYGIENE ON HOME COMPUTERS

Ensuring proper IT hygiene practices is one of the best ways to secure your workforce. Attack surface reduction through hardening and proper configuration before a machine is used for business purposes is standard practice. The use of personal computers for working from home, however, means that security and IT teams don't necessarily have the chance to ensure that these preventative measures are in place.

As a result of IT hygiene issues, remote employees might be working with dangerous unhardened systems with an increased attack surface. Further, they might be working with vulnerable applications that leverage high privileges without the IT team's knowledge.

80% of successful attacks are new or unknown zero days

Source: Ponemon Institute

HOW MOVING TARGET DEFENSE FIXES THE PROBLEM

Morphisec provides instant hardening for endpoints without the need for manual configuration. Patented Moving Target Defense technology dismantles the attack pathways to drastically reduce the attack surface of every machine it protects. Morphisec's prevention capabilities do not depend on updates or configuration policies; protection is in place the moment the agent is installed.

Morphisec provides a mitigating technology that qualifies as a compensating control for compliance purposes. With Morphisec, organizations can extend their virtual patching cycles yet reduce risk. IT departments can rely on moving target defense to prevent exploits on vulnerable applications with high privileges.

CONCLUSION

The remote work trend is not likely to abate anytime soon. As more employees work from home, and more organizations realize the financial and productivity benefits—OpenVPN found that enterprises can save $11,000 a year per employee by having them work remotely—IT and security teams will face additional challenges around ensuring long-term security.

That's why the Morphisec Unified Threat Prevention Platform is so powerful. Its moving target defense technology protects remote workers no matter the reliability or security of their home network, ensuring that critical data is protected against cyberattack and remote employees can access the data they need to do their work.

ABOUT MORPHISEC

Morphisec delivers an entirely new level of innovation to customers with its patented Moving Target Defense technology - placing defenders in a prevent-first posture against the most advanced threats to the enterprise, including APTs, zero-days, ransomware, evasive fileless attacks and web-borne exploits. Morphisec provides a crucial, small footprint memory-defense layer that easily deploys into a company's existing security infrastructure to form a simple, highly effective, cost-efficient prevention stack that is truly disruptive to today's existing cybersecurity model.

f in 🐦

MORPHISEC
Moving Target Defense